개정이력

차수	재(개)정 일자	시행일자	주요 개정 내용
1	2025-01-07	2025-01-07	초도 제정

목 차

1. 개요

1.1 목적

본 지침서는 정보보안침해사고에 대한 대응 및 복구업무를 포함하며, 피해를 최소화하고 재발방지를 통하여 정보자산의 보안성과 안정성을 유지하는데 필요한 사항을 규정하는데 목적을 둔다.

1.2 적용범위

사내 모든 IT자산과 이를 관리하는 운영 담당자 및 모든 임직원을 대상으로 한다.

1.3 책임 및 권한

1.3.1 CSO

1) 보안침해사고 발생시 점검 및 분석결과를 확인하고 보안사고 처리를 주관한다.
2) 보안침해사고 목록을 유지, 관리하며 예방을 위한 정기적인 교육을 실시한다.
3) 필요시 대외기관에 통보 및 협력한다.

1.3.2 모든 임직원

1) 회사에 근무하는 모든 인력은 허가된 범위내에서 정보자산을 이용할 수 있는 권한이 있으며,
2) 불법사용에 의한 보안사고의 최종 책임은 해당 임직원에게 있다.
3) 보안침해사고 발생 또는 사고징후 발견시 임의로 문제 해결을 시도해서는 안되며, 해당 부서의 장 또는 CSO에 즉시 통보하여야 한다.

1.4 조직

1.4.1. 정보보안 침해사고 대응을 위해 CSO, 정보보안그룹, 각 부서 보안담당자로 구성된 사고대응팀을 조직한다.

1.5 역할

1.5.1 CSO : 전사 보안사고에 대한 총괄 책임- 외부 기관 보고 및 대외 협력 주관

1.5.2 정보보안그룹 : 시스템 및 네트워크 로그 수집, 분석 지원- 기술적 차단 및 복구 조치 수행

1.5.3 부서 보안담당자 : 각 부서 보안사고 접수 및 1차 보고 담당- 사용자 교육 및 인식 제고 역할 수행

2. 보안침해사고 예방

2.1 시스템 보안성 검토

2.1.1 시스템 도입, 변경, 폐기시 보안성 검토를 실시하여 보안상 이슈를 사전에 제거한다.

2.2 취약점 점검 및 조치

2.2.1 불필요한 계정은 삭제하거나 계정을 차단하고 패스워드가 없는 계정은 패스워드 설정을 하여 조치를 취한다.

2.2.2 최근의 해킹 방법 및 대처방안에 대한 자료를 입수하여 대비한다.

2.2.3 주요 보안 이슈가 발생할 경우 긴급 조치사항을 배포하여 문제발생을 사전에 대처하도록 한다.

3. 보안침해사고 감지 및 대응

3.1 보안침해사고 감지

3.1.1 정보보안그룹은 다음과 같은 징후가 감지되면 확인 및 점검 후 보안침해사고로 판단될 시에 CSO에게 즉각 보고 후 대응한다.

1) 악성코드의 공격으로 판단되는 경우
2) 네트워크에 과도한 부하를 발생시키는 프로그램이 실행되는 경우
3) 파일, 서비스 또는 기타 자원에 비인가 접근시도가 발견되는 경우
4) 보안 관련 파일의 수정 및 관리자 권한 외의 작업수행 시도가 발견되는 경우
5) 계정관련 시스템에 관리자 이외의 접근 시도가 발견되는 경우
6) 기타 이상 징후가 발견되는 경우

3.1.2 일반 사용자가 다음과 같은 징후를 발견하는 경우 가능한 빠른 시간 내에 CSO 또는 해당 부서장에게 보고한다.
1) 사용자 PC의 비정상적인 활동이나 징후가 바이러스, 웜 등의 악성코드 공격으로 판단되는 경우
2) 회사 정보 시스템 사용 중 해킹의 흔적을 발견하는 경우
3) 본인의 계정이 도용된다는 의심이 발견되는 경우
4) 다른 임직원이 내부에서 보안침해사고 행위 발견 및 징후 발생시

3.1.3 외부 단체나 외부인에게 허가 없이 보안 사고를 통보하는 것을 금한다.

3.2 보안침해사고 대응

3.2.1 이상징후 발견시 보안침해사고인지 장애와 같은 다른 사유로 발생하였는지를 판단한다.
3.2.2 보안사고로 확인될 경우 원인분석 전에 피해시스템에 대한 백업을 실행한다.
3.2.3 내부 단말기에서 침투한 경우 현재의 단말 위치를 확인한다.
3.2.4 가능한 도구나 명령어를 이용하여 침입자에 관련된 정보를 수집한다.
3.2.5 침입자가 수행하고 있는 명령어를 파일로 저장하거나 기록한다.
3.2.6 보안침해사고로부터 시스템 보호가 우선시 되는 경우 네트워크 접속을 차단하고 불가피할 경우 해당 시스템의 서비스를 중지해야 한다.
3.2.7 보안침해사고 발생 및 대응은 CSO에게 즉각적으로 보고되어야 한다.
3.2.8 보안침해사고 로그를 저장해야 하며 침입자의 추적이 필요시 CSO의 동의하에 외부 유관업체와 협력하여 대응하여야 한다.

3.3. 대응절차

3.3.1 이상징후 감지 → 긴급조치 → 원인분석 → 복구조치 → 사후보고 및 예방대책 수립의단계로 대응한다.

4. 보안침해사고 처리 및 사후조치

4.1 보안침해사고 처리 후 점검사항

4.1.1 각종 시스템의 로그를 분석하여 시스템 침입 흔적 및 변경 유무를 확인한다.
4.1.2 숨겨진 비인가 파일 및 Backdoor 등 악성코드 설치여부를 확인한다.
4.1.3 새로운 계정 생성 유무 및 패스워드 변경 여부를 확인한다.
4.1.4 보안침해사고 피해 정도를 파악하여 정보자산의 보안성이 손상되었을 경우 즉시 백업파일을 이용하여 복구하여야 한다.
4.1.5 보안침해사고 처리 후 취약점 점검을 수행하여 안전하다고 판단되는 경우 서비스하도록 한다.

4.2 사후조치

4.2.1 CSO는 임시 조치된 문제에 대해서는 근본 해결책을 강구하고, 추후 재발방지를 위한 대응책을 마련한다.
4.2.2 공개가 허용된 보안침해사고는 임직원에게 공지 또는 교육하여야 한다.

4.2.3 보안침해사고에 대해 시정 조치가 종료될 때까지 모든 기록을 유지, 관리하여야 한다.

4.2.4 보안침해사고의 법적 대응에 대비하여 침해증거 수집 및 보관을 하여야 하며, 보관된 자료는 변조가 되지 않도록 한다.

4.2.5 사고의 원인이 내부자의 소행으로 드러날 경우 사규에 의거 인사조치를 하여야 한다.

4.2.6 보안침해사고나 취약점에 대한 승인되지 않은 정보의 사외유출을 금지한다.